

Hackende hacker gehackt

In het novembern timer van **informatie** (nr. 9, 2005) gaf ik een impressie hoe kinderlijk eenvoudig het is om in te breken op computersystemen via de vele onzorgvuldig gebouwde webapplicaties die erop draaien. Van verschillende kanten vernam ik dat het kind in velen wakker geworden was en men mijn spoedcursus SQL injection attacks in de praktijk probeerde te brengen. Het 13-jarige zontje van de hoofdredacteur van **informatie** was druk bezig geweest, met enig succes naar ik begreep. Van anderen hoorde ik ook dat men driftig aan het hacken geslagen was.

In de paragraaf 'Inloggen zonder wachtwoord' had ik aangegeven hoe je snel en simpel voorbij langdradige loginprocedures komt. In het kort komt het hierop neer: adjungeer een immer ware uitspraak aan een willekeurige login en dito wachtwoord. Doe dat met een OR, zodat de hele bewering waar wordt, en je bent binnen.

Ik herinner me nog goed dat de hoofdredacteur graag wilde dat de spoedcursus ook heus bewijs zou bevatten, dus een recente SQL-attack op een ziekenhuis kwam goed van pas. Achteraf bleek dat we veel dichterbij huis hadden kunnen blijven getuige een heel aardige reactie die ik kreeg van een oplettende lezer die zijn geluk had beproefd op de website van het blad **informatie** zelf.

Op archieff.informatie.nl wordt u vriendelijk verzocht uw abonneenummer in te vullen om toegang te verkrijgen tot het online archief van **informatie**, dat is voorbehouden aan de abonnees van **informatie** en de leden-abonnees van het NGI en het SAI. Bespaar uzelf het zoeken naar de wikkel van **informatie** of het lidnummer dat op de automatische betaling van uw lokale informaticaclub staat, maar tik gewoon in: ` OR "1=1" en klik op OK. Jawel, u bent meteen binnen en u kunt nog eens nalezen hoe dit precies werkt door het artikel 'Hacken doe je zo' uit het nu gratis toegankelijke archief op te halen (inmiddels niet meer mogelijk, red.).

Informatie.nl hacken is als spioneren bij de AIVD, stelen van de politie of brand stichten in de kazerne. Dus eigenlijk is het te gek om los te lopen dat bij een vakblad voor it-professionals de zaakjes niet op orde zijn. Gelukkig kon de hoofdredacteur hier ook wel weer de humor van inzien, en ik begrijp dat er een nieuwe website gaat komen. Dit beveiligingslek zal er dan wel uit zijn, maar het biedt weer mogelijkheden voor nieuwe kwetsbaarheden.

Dat overkwam degene die me mailde: hij bleek geen doorgewinterde hacker, sterker, hij was zelf net gehackt. 'BIOS Ownz U' prijkte als hackerstrofee op zijn website. En wederom was het probleem terug te voeren op het ontbreken van inputvalidatie op een cruciale plek in de code. Hoogstwaarschijnlijk werd de site gehackt doordat het via een trucje mogelijk was PHP-commando's uit te voeren op de doelserver; een lek in het onderliggende softwarepakket, dat gebruikmaakt van PHP. PHP is een recursief acroniem dat 'PHP: Hypertext Preprocessor' betekent. PHP is een veelgebruikte open-sourcescripttaal die je met HTML-pagina's kunt mixen om allerlei leuke dingen te doen. Een van die leuke dingen is om distributed computing over het internet te laten verlopen. De commando's worden verzonden via het HTTP-protocol voor websites en die verpak je in XML-formaat. Een soort alles-met-allesverbinder die geen last heeft van verschillende besturingssystemen, verschillende omgevingen, verschillende talen en security. Alleen dat laatste staat er niet bij in de 'open-soresfolder'.

De gewraakte code wordt gebruikt in een groot aantal populaire webpakketten, waar ook de gehackte hacker gebruik van maakte. Jammer genoeg bleek het mogelijk op afstand code te laten runnen via deze ultraflexibele extensie boven op PHP, zonder welke je niet kunt leven, dat spreekt. Een simpele check via Google laat zien dat er momenteel meer dan twintigduizend hits zijn waarin 'Ownz U' te vinden is, en naar het zich laat aanzien wordt er willekeurige webcontent neergezet op kwetsbare sites. De hoofdpagina vervangen, stukjes tekst invoegen, extra pagina's toevoegen, hele sites onklaar maken, sites vervuilen met lange rijen error logs, enzovoort. En wie draait daarvoor op?

Uiteraard is de open-sourcegemeenschap snel met het verbeteren van fouten, zodat de ellende in de nieuwe versie snel tot het verleden behoort. In de praktijk van alledag is het echter zo dat veel eigenaren van websites geen idee hebben wat hen overkomt door alle 'hacktiek', en dat het voor hen niet zo gemakkelijk is na te gaan wat hier is gebeurd, laat staan wat je eraan moet doen.

Het is dan ook niet voor niets dat je voor gebruik de aanwijzingen op de verpakking moet lezen. Als we dat doen voor de klonterende allesbinder, blijkt die over de PHP-licentie te beschikken. En die licentie vertelt ons dat het PHP-ontwikkelteam zijn programmeervruchten als is ter beschikking stelt, en dat zelfs geschiktheid voor een bepaald doel wordt ontkend: '[...] Any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed'. Open source in optima forma.

Gebruikmaken van software met onbekende kwaliteitskenmerken of softwareontwikkelaars met onbekende kwaliteitsattributen leidt onherroepelijk tot ellende. Of het nu defacing van websites is of het gratis meelesen met het blad **informatie**.

Prof. dr. Chris Verhoef

is hoogleraar Informatica bij de afdeling Informatica van de Vrije Universiteit Amsterdam. E-mail: x@cs.vu.nl.